United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Mike Swift
MLex Market Intelligence
324 Metzgar Street
Half Moon Bay, CA 94019

FEB 13 2013

Re: FOIA-2013-00197
Facebook

Dear Mr. Swift:

This is in response to your request dated November 28, 2012 under the Freedom of Information Act seeking access to documents regarding the 90-day Facebook compliance report. In accordance with the FOIA and agency policy, we have searched our records, as of November 28, 2012, the date we received your request in our FOIA office. We have located the responsive record which is granted in full and is enclosed.

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington D.C. 20580 or by facsimile at (202) 326-2477, within 30 days of the date of this letter. Please enclose a copy of your original request and a copy of this response.

If you have any questions about the way we are handling your request or about the FOIA regulations or procedures, please contact Elena Vera at (202) 326-3368.

Sincerely,

Dione J. Stearns
Assistant General Counsel

Enclosed:
15 pages

facebook

Submitted to: Debrief@ftc.gov

Associate Director of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580

November 13, 2012

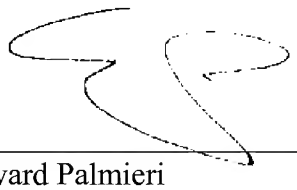
Re: In the Matter of Facebook, Inc., FTC Docket No. C-4365

To the Associate Director of Enforcement:

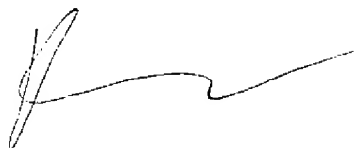
Facebook Inc. ("Facebook") submits the attached Report pursuant to Part IX of the Decision and Order, served on Facebook on August 15, 2012 (the "Order"). The Report describes the manner and form in which Facebook is in compliance with the Order. The Report follows the outline of the Order paragraph by paragraph.

Please do not hesitate to contact us if you have any questions.

Sincerely,



Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.



Daniel Li
Product Counsel
Facebook, Inc.

1601 Willow Road, Menlo Park, California 94025
650.543.4800 - tel 650.543.4801 - fax

In the Matter of	)	
FACEBOOK, INC.,	)	**DOCKET NO. C-4365**
a corporation.	)	

Facebook Compliance Report

This report (this "Report") sets forth the manner and form in which Facebook, Inc. ("Facebook") is in compliance with the Decision and Order, served on Facebook on August 15, 2012 (the "Order"). This Report is prepared and filed with the Federal Trade Commission (the "Commission") pursuant to Part IX of the Order. This Report follows the outline of the Order paragraph by paragraph.

I.

Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

- **A. its collection or disclosure of any covered information;**
- **B. the extent to which a consumer can control the privacy of any covered information maintained by Respondent and the steps a consumer must take to implement such controls;**
- **C. the extent to which Respondent makes or has made covered information accessible to third parties;**
- **D. the steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;**
- **E. the extent to which Respondent makes or has made covered information accessible to any third party following deletion or termination of a user's account with Respondent or during such time as a user's account is deactivated or suspended; and**
- **F. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework.**

Facebook describes the extent to which it maintains the privacy and security of covered information in its Data Use Policy (the "Data Use Policy"), available at https://www.facebook.com/full_data_use_policy. The Data Use Policy is drafted in a layered, web-like format, which makes its description of Facebook's data collection and disclosure practices easy to navigate. It is drafted in plain and simple language, conspicuously labeled, and formatted in a font that is easily read. It is available in many of the languages used by the

people who access and share on Facebook.

The Data Use Policy addresses the following topics: 1) Information Facebook receives and how the information is used; 2) Sharing and finding users on Facebook; 3) Other websites and applications; 4) How advertising and sponsored stories work; 5) Cookies, pixels, and other system technologies; and 6) Some other things users need to know. Facebook has designated a member of its Legal team to be responsible for maintaining the Data Use Policy.

Facebook's Data Use Policy was last updated on June 8, 2012. The date of the last revision is clearly provided at the beginning of the Data Use Policy so that a user can determine whether the Data Use Policy has changed since the user's last review of the Data Use Policy.

Facebook's comprehensive privacy program, described in Part IV of this Report (the "Privacy Program"), is reasonably designed to ensure that Facebook does not misrepresent the extent to which it maintains the privacy or security of covered information as set forth in Section I of the Order.

Specifically, as part of the Privacy Program, Facebook built an extensive privacy review process that is supervised and monitored by, among others, Facebook's Chief Privacy Officer, Policy and Facebook's Chief Privacy Officer, Product. This process is designed to integrate a detailed and multi-faceted privacy review into the early development stages of a new product or material product upgrade and to continue that review throughout the product's life cycle. This ongoing privacy review is designed to conform newly released and existing products with the Data Use Policy and other Facebook representations and to revise Facebook's user-facing statements as necessary to reflect the evolution of its products and ecosystem. The privacy review process involves comprehensive review by a cross-functional team of Facebook employees that includes representatives from major segments of Facebook, including Facebook's Privacy, Public Policy, Legal, Marketing, Product, Engineering, Security, and Communications teams (the "Privacy Cross-Functional Team"). The Privacy Cross-Functional Team reviews Facebook products, services, policies, and related disclosures.

In addition, as part of the Privacy Program, Facebook is implementing comprehensive privacy training for all Facebook employees to augment existing group-specific training (e.g., privacy training for new Product Managers), with the goal of educating all Facebook employees about Facebook's privacy policies and representation obligations. Facebook also has dedicated personnel in its Legal department who focus on spotting, vetting, and addressing privacy issues and disclosures.

Facebook has been careful to detail changes in the manner it shares information, even with respect to information that is outside the scope of the Order. For example, on September 30, 2012, Facebook's Privacy Engineer published a blog post titled "Relevant Ads That Protect Your Privacy" concerning targeted advertising, which comprehensively addressed changes in the way Facebook targets ads to users. The blog post is available at https://www.facebook.com/notes/facebook-and-privacy/relevant-ads-that-protect-your-privacy/457827624267125. In addition, Facebook recently added privacy education to its new user experience, with the aim of educating Facebook users about how privacy works on Facebook.

II.

Respondent and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic user information by Respondent with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:

A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and

B. obtain the user's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this order; or (2) require Respondent to obtain affirmative express consent for sharing of a user's nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user's privacy setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

Facebook's Privacy Program is designed in part to identify changes that fall under the scope of Part II of the Order and to implement the disclosure and consent requirements of Part II of the Order, where applicable. The specific policies and procedures mentioned in Part I of this Report and described in more detail in Part IV of this Report—including compliance oversight by Facebook's two Chief Privacy Officers, review of developing products and services by the Privacy Cross-Functional Team, new and continuing employee training, and dedicated privacy-focused Legal personnel—all contribute to identifying new or changed products or services that may trigger the disclosure and consent requirements of Part II of the Order. The Privacy Cross-Functional Team plays a central role in discussing and providing recommendations to the Chief Privacy Officers with respect to whether the disclosure and consent requirement of Part II of the Order may be triggered by a particular product or change.

In addition, to help communicate the requirements in Part II of the Order, Facebook has distributed a copy of the Order to all Facebook employees and has implemented a global process to similarly distribute the Order to all new employees—steps that go beyond the requirements of Part VII of the Order.

Facebook continues to monitor and evaluate proposed changes (if any) to users' privacy settings to ensure compliance with Part II of the Order.

III.

Respondent and its representatives, in connection with any product or service, in or affecting commerce, shall, no later than sixty (60) days after the date of service of this order, implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its users from fraud or illegal activity. Nothing in this paragraph shall be construed to require Respondent to restrict access to any copy of a user's covered information that has been posted to Respondent's websites or services by a user other than the user who deleted such information or deleted or terminated such account.

Facebook has implemented procedures to comply with Part III of the Order. Specifically, Facebook has implemented a Data Deletion and Retention Framework (the "Data Deletion and Retention Framework"), which outlines the retention period for specific types of data, in all cases in compliance with Part III of the Order. Facebook has also undertaken a historical deletions project, which covers content created prior to implementation of the Data Deletion and Retention Framework. The Data Deletion and Retention Framework ensures that when a user deletes his or her Facebook account, the appropriate user data associated with that account is deleted (subject to any legal obligation to retain data). It also ensures that when a user deletes content, the appropriate content is deleted from Facebook's permanent data stores within a reasonable period of time. The Data Deletion and Retention Framework goes beyond the requirements of Part III of the Order, which focuses only on accessibility by third parties, rather than deletion.

Part III of the Order was a response to reports that some images stored on one of Facebook's old photo storage systems remained accessible after users had deleted the images, where users had retained a unique URL associated with the image. Facebook addressed this issue earlier this year by migrating all of its stored photos to a new storage system ("Haystack"[1]) and decommissioning the old photo storage system. Facebook completed the migration to Haystack in July 2012. Haystack controls access to all photos that are served to content delivery networks. It ensures that each photo that is delivered to a content delivery network has a lifespan of 30 days or less. When a photo is deleted by a user, Facebook refuses to provide the photo to any content delivery network that requests it after the moment of deletion. The system is thus designed to ensure that, once the lifespan of the photo expires, it will not be visible via any content delivery network that received the photo previously.

With respect to other covered information, Facebook has comprehensive procedures for deleting information that has been deleted by users and ensuring that it cannot be accessed by third parties from servers under Facebook's control after a reasonable period of time. In addition, Facebook has implemented controls to ensure that any issues that arise with respect to data deletion are identified and addressed.

Facebook has a comprehensive, reliable system for deleting accounts that users have

---

[1] *See* Peter Vajgel, *Needle in a Haystack: Efficient Storage of Billions of Photos*, FACEBOOK, April 30, 2009, https://www.facebook.com/note.php?note_id=76191543919.

terminated. Facebook performs systematic checks on deleted accounts to ensure that its Data Deletion and Retention Framework is operating properly, and it escalates any issues to the appropriate teams.

Facebook's Engineering teams are responsible for building and maintaining the core systems that comprise the Data Deletion and Retention Framework. Any identified issues are raised to Facebook's Security Infrastructure personnel.

IV.

Respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including:

Facebook has taken extensive steps to establish, implement, and maintain the Privacy Program, which is documented in written policies and procedures. Facebook has selected the AICPA and CICA Generally Accepted Privacy Principles ("GAPP") framework as the foundation for its Privacy Program and supporting controls. There are 10 GAPP principles, which are derived from internationally recognized information practices and privacy laws and regulations from around the world. The 10 GAPP principles are:

1. Management. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

2. Notice. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

3. Choice and consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4. Collection. The entity collects personal information only for the purposes identified in the notice.

5. Use, retention, and disposal. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

6. Access. The entity provides individuals with access to their personal information for review and update.

7. Disclosure to third parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. Security for privacy. The entity protects personal information against unauthorized access (both physical and logical).

9. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

10. Monitoring and enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.[2]

In March 2012, Facebook engaged a professional services firm to assess Facebook's Privacy Program against the GAPP framework and provide observations and recommendations for future enhancement of Facebook's Privacy Program.

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

Facebook has designated specific employees to coordinate and be responsible for the Privacy Program, which is led by the Chief Privacy Officer, Product. Key stakeholders in the Privacy Program include the Chief Privacy Officer, Product; the Chief Privacy Officer, Policy; two Associate General Counsels, Privacy; Regulatory Counsel; and the Chief Security Officer (the "Privacy Governance Team").

While the Chief Privacy Officer, Product provides leadership responsibility for coordinating the Privacy Program, the Privacy Governance Team and many employees are responsible for various aspects of—and are integral to—the Privacy Program. Facebook's Chief Privacy Officer, Product and his team are integrated into the product development process and lead Facebook's commitment to build privacy into its products at an early stage of development. The Privacy Cross-Functional Team meets weekly to review all new products and product changes documented by the Chief Privacy Officer, Product and his team. Members of the Privacy Cross-Functional Team also engage in ongoing review efforts independent of the weekly meetings.

In addition, Facebook's Legal team includes a number of attorneys who serve as primary legal counsel for new products and services. These attorneys are responsible for ensuring that any new or revised products or services are consistent with Facebook's disclosures and comply with applicable legal requirements. These attorneys also support the Privacy Cross-Functional Team and participate in the Privacy Program.

Under the Privacy Program, Facebook considers privacy at all stages of the product cycle and empowers Facebook employees to take ownership over privacy issues, under the leadership

---

[2] AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, INC. AND CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, GENERALLY ACCEPTED PRIVACY PRINCIPLES 7 (2009).

of the Privacy Governance Team.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

A subgroup of the Privacy Governance Team has worked to evaluate Facebook's privacy risks. That process has resulted in a privacy risk assessment and an ongoing process aimed at identifying reasonably foreseeable, material risks, both internal and external. As part of Facebook's privacy risk assessment process, members of Facebook's Legal team interviewed relevant Facebook stakeholders, including representatives of Facebook's Privacy, Engineering, Security, Internal Audit, Legal, Finance, Platform Operations, and User Operations teams. This process identified key internal and external risks that could result in the unauthorized collection, use, or disclosure of covered information.

The discussions considered risks in each relevant area of operation, including governance, product design and engineering (including product development and research), user operations (including third-party developers), advertisers, service providers, employee training and management (including training on the requirements of the Order), and security. The discussions also included an assessment of the sufficiency of the controls in place to control the identified risks. Facebook leveraged previous audits and assessments to identify possible areas of risk exposure, as well as existing controls that help to mitigate the identified risks. Based on this process, Facebook documented its risk assessment and mapped its existing privacy controls to the GAPP framework, as described in more detail below in Part IV.C of this Report.

As part of Facebook's privacy risk assessment process, Facebook will hold an annual "Privacy Summit" of relevant stakeholders, including key representatives from the Privacy Cross-Functional Team. The attendees of the annual Privacy Summit will review and update the privacy risk assessment, which will include evaluating privacy risks in light of changing internal and external risks, changes in operations, and changes in laws and regulations. They will also consider the sufficiency of existing controls in mitigating identified risks and will project forward over the upcoming year to forecast new potential privacy risks. The privacy risk assessment will be updated as a result of any new or revised risks identified at the Privacy Summit. Any control recommendations will be escalated as appropriate. The next Privacy Summit is currently scheduled for January 2012.

C. the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedures.

Facebook has performed a granular mapping of its existing privacy controls to the GAPP framework. Facebook assessed each GAPP criteria to determine if the controls in place adequately controlled for the associated risks; it identified certain controls that had room for enhancement; and it implemented remediation plans with respect to those controls.

These processes resulted in the documentation of a mapping of Facebook's controls to the GAPP framework, along with the status of each control. Facebook has implemented remediation steps for the majority of controls where remediation was recommended, and is in the process of implementing remediation steps for a small number of remaining controls. Facebook will continue to refine and implement reasonable controls and procedures to address identified privacy risks on an ongoing basis and will regularly monitor the effectiveness of its controls and procedures.

In order to ensure that the effectiveness of its controls and procedures are regularly monitored, Facebook has designated an "owner" for each one of the controls included in the Privacy Program. Facebook will also utilize the annual Privacy Summit to monitor the effectiveness of controls and procedures in light of changing internal and external risks. In addition, a member of Facebook's Legal team will perform an annual review of the Privacy Program to ensure that the Privacy Program, including the controls and procedures contained therein, remains effective. This Legal team member will update the Privacy Program to reflect any changes or updates communicated by employees of Facebook. This member of the Legal team also serves as the point of contact for all control "owners." The control owners reach out to the Legal point of contact with issues or updates to their respective controls.

Privacy Training

Facebook conducts privacy-related training and is in the process of implementing a comprehensive training program to further extend the audience and topics covered and to further promote recognition and understanding of privacy issues among Facebook employees, including awareness of Facebook's obligations under the Order. All new employees will be required to undergo privacy training within 30 days of their first day of employment at Facebook. All existing Facebook employees will be required to refresh the privacy training on an annual basis. At the time of the annual privacy training, Facebook employees will be required to confirm their understanding of Facebook's privacy practices. Facebook has devoted considerable resources to its employee training program, including engaging an external firm that has expertise in delivering high-impact content.

Facebook has already delivered a copy of the Order to all existing employees and has established a process to similarly distribute the Order to all new employees. Employees are encouraged to review the Order and to direct any questions to a point of

contact in the Legal team.

Product Design, Development, and Research

Facebook has designed its product-review process to enable the Privacy Cross-Functional Team to consider privacy from the earliest stages in the product development process. The Chief Privacy Officer, Product and his team spearhead this review and lead a number of key functions and responsibilities. First, they educate employees, including Engineers, Product Managers, Content Strategists, and Product Marketing Managers, on Facebook's privacy framework. This includes an overview of Facebook's processes and corresponding legal obligations, and may involve other members of the Privacy Cross-Functional team, such as Privacy Counsel.

Second, the Chief Privacy Officer, Product and his team host weekly reviews of key product-related privacy decisions and material changes to Facebook's privacy framework, which are attended by members of the Privacy Cross-Functional Team. The Chief Privacy Officer, Product and his team also review all new products and material product changes from a privacy perspective and involve the Privacy Cross Functional Team for broader review and feedback. Product launches are added to the launch calendar to ensure review and consideration of privacy issues by the Privacy Cross-Functional Team. Members of the Privacy Cross-Functional Team also communicate back to their respective teams on issues covered in the weekly reviews. The goal of this process is to ensure that privacy is considered throughout the product development process, and to maintain consistency on privacy issues across all Facebook products and services.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.

Where appropriate, Facebook has implemented controls with respect to service providers, including implementing policies to select and retain service providers capable of appropriately protecting the privacy of covered information received from Facebook.

Facebook's Security team has a process for conducting due diligence on service providers who may receive covered information, in order to evaluate whether the service providers' data security standards are in-line with Facebook's commitments to protect covered information. As part of the due diligence process, Facebook may ask prospective service providers to complete a security architecture questionnaire to assess whether the provider meets Facebook's functional security requirements. The process can also involve Facebook sending potential service providers a vendor security questionnaire that provides Facebook with detailed information on the service provider's security posture, including information on protecting the privacy of customer data. Based upon the service provider's responses to the vendor security questionnaire and other data points, Facebook's Security team determines whether further security auditing may be required.

When the Security team determines further auditing is required, Facebook partners with an outside security consulting firm to conduct a security audit on the potential service provider in order to determine whether the service provider meets Facebook's security requirements. Depending on the particular service provider, this audit may include testing of the service provider's controls, a vulnerability scanning program, a web application penetration test, and/or a code review for security defects. The security consulting firm then reports its findings to Facebook, and Facebook requires service providers to fix critical issues before the service provider is on-boarded. Once the issues are fixed, Facebook Security may ask the security consulting firm to re-test the service provider to make sure the identified issues were resolved according to Facebook's standards.

Depending upon the nature of Facebook data shared with the service provider and other factors, Facebook may require the service provider to undergo a periodic security audit. Facebook also conducts random security audits (logical, network, and/or physical) on selected service providers to assess their compliance with Facebook's security guidelines.

Additionally, in January 2012, Facebook implemented a contract policy (the "Contract Policy"), which governs the review, approval, and execution of contracts for Facebook. It is designed to provide an effective means for establishing contracts while maintaining appropriate internal controls and managing risks associated with entering into and amending contracts. Among other things, the Contract Policy specifies that Facebook contracts must comply with applicable Facebook policies.

The Contract Policy communicates Facebook's preference to enter into contracts on its pre-approved standard contract templates. Facebook's pre-approved contract templates require service providers to implement and maintain appropriate protections for covered information. Facebook reviews contracts that deviate from the pre-approved templates to help ensure that contracts with applicable service providers contain the required privacy protections. Facebook Legal evidences review of any such contracts through formal approval prior to contract execution.

E. the evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

Facebook's Privacy Program is designed with procedures for evaluating and adjusting the Privacy Program in light of the results of testing and monitoring of the program as well as other relevant circumstances. Facebook's annual Privacy Summit is designed to identify, discuss, and assess compliance with privacy policies and procedures, and applicable laws and regulations, as well as identify new or changed risks and recommend responsive controls. The Privacy Program will be adjusted based upon the recommendations derived from the Privacy Summit. The Privacy Summit is attended by relevant stakeholders, which ensures that input is received from appropriate teams throughout Facebook.

In addition, a member of Facebook's Legal team maintains the Privacy Program and serves as a point of contact for all "owners" of the controls that are currently in place. Such "owners" communicate to the Legal point of contact any recommended adjustments to the Privacy Program based upon their regular monitoring, as well as any internal or external changes that affect the controls in question. The point of contact from Facebook's Legal team adjusts the Privacy Program on an annual basis based upon such input. The Privacy Cross-Functional Team also assesses risks and controls on an on-going basis through weekly meetings and review processes. Any recommendations for adjustments to the Privacy Program are raised to the point of contact in the Legal team.

V.

In connection with its compliance with Part IV of this order, Respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such Assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, in his or her sole discretion. Any decision not to approve a person selected to conduct such Assessments shall be accompanied by a writing setting forth in detail the reasons for denying such approval. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- **A. set forth the specific privacy controls that Respondent has implemented and maintained during the reporting period;**
- **B. explain how such privacy controls are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information;**
- **C. explain how the privacy controls that have been implemented meet or exceed the protections required by Part IV of this order; and**
- **D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.**

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate

Director of Enforcement within ten (10) days of request.

Facebook is in the process of selecting a qualified third-party professional to prepare the Assessments required by Part V of the Order, which Facebook will identify to the Associate Director for Enforcement for approval, in accordance with Part V of the Order.

VI.

Respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different privacy setting made available to users;

Facebook maintains and will make available to the Commission the enumerated statements, materials and documents in Part VI.A of the Order upon request, so long as such documents are responsive and non-privileged.

B. for a period of six (6) months from the date received, all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

Facebook maintains and will make available to the Commission the enumerated statements, materials, and documents in Part VI.B of the Order upon request, so long as such documents are responsive and non-privileged.

C. for a period of five (5) years from the date received, any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this order;

Facebook maintains and will make available to the Commission the enumerated statements, materials, and documents in Part VI.C of the Order upon request, so long as such documents are responsive and non-privileged.

D. for a period of three (3) years from the date of preparation or dissemination, whichever is later, each materially different document relating to Respondent's attempt to obtain the consent of users referred to in Part II above, along with documents and information sufficient to show each user's consent; and documents sufficient to demonstrate, on an aggregate basis, the

number of users for whom each such privacy setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent; and

Facebook shall maintain and will make available to the Commission the enumerated statements, materials, and documents in Part VI.D of the Order upon request, so long as such documents are responsive and non-privileged.

E. for a period of three (3) years after the date of preparation of each Assessment required under Part V of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

Facebook shall maintain and will make available to the Commission the enumerated statements, materials, and documents in Part VI.E of the Order upon request, so long as such documents are responsive and non-privileged.

VII.

Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VIII. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VIII, delivery shall be at least ten (10) days prior to the change in structure.

On September 12, 2012, Facebook timely delivered a copy of the Order to all Facebook employees—not just the Facebook employees indicated in Part VII of the Order. Separate delivery of the order was made the same day to each member of Facebook's Board of Directors. In addition, Facebook has established a process to similarly distribute the Order to all new employees. Employees are encouraged to review the Order and to direct any questions to a point of contact in the Legal team.

VIII.

Respondent shall notify the Commission within fourteen (14) days of any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Unless otherwise directed by a representative of the Commission, all notices required by this Part

shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of Facebook, Inc.*, Commission File No.[ ]. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@Commission.gov.

Facebook shall notify the Commission, in accordance with Part VIII of the Order, should any of the triggering events described in Part VIII occur.

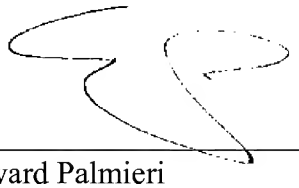
IX.

Respondent, within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, Respondent shall submit additional true and accurate written reports.

This Report satisfies the requirement under Part IX of the Order to file a report with the Commission within 90 days after the date of service of the Order.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

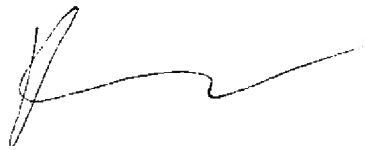
Executed on November 13, 2012



Edward Palmieri
Associate General Counsel, Privacy
Facebook, Inc.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on November 13, 2012



Daniel Li
Product Counsel
Facebook, Inc.